DOI:10.24996/ijs.2018.59.4A.18

ISSN: 0067-2904

Some application of coding theory in the projective plane of order three

Najm A. M. AL-Seraji*, Raad I. K. AL-Humaidi
Department of Mathematics, College of Science, University of Mstansiriyah, Baghdad, Iraq

Abstract

The main aim of this paper is to introduce the relationship between the topic of coding theory and the projective plane of order three. The maximum value of size of code over finite field of order three and an incidence matrix with the parameters, n (length of code), d (minimum distance of code) and e (error-correcting of code) have been constructed. Some examples and theorems have been given.

Keywords: projective plane, coding theory, incidence matrix.

حول تطبيق نظرية الترميز للمستوي الاسقاطي من الرتبة الثالثة

نجم عبد الزهره مخرب السراجي*، رعد ابراهيم خويط الحميدي
قسم الرياضيات ، كلية العلوم ، الجامعة المستنصرية ، بغداد، العراق

الخلاصة

الهدف الرئيسي لهذا البحث هو تقديم العلاقة بين موضوع نظرية الترميز و المستوي الاسقاطي من الرتبة الثالثة . القيمة العظمى لحجم الرمز M حول الحقل المنتهي من الرتبة الثالثة ومصفوفة الاصابة مع المعلمات n (طول الرمز)، d (اقل مسافة للرمز) و e (تصحيح رمز الاخطاء) تم تشكيلها . بعض الامثلة والنظريات أعطيت.

1. Introduction

The subject of this research depends on themes of

- Projective geometry over a finite field;
- Group theory;
- Linear algebra;
- Field theory;
- Coding theory.

The summary history of this theme is shown as follows:

- All theorems and definitions of the research are taken from James Hirshfeld [1];
- In 1986. R. Hill. [2] introduced the fundamental concepts and facts on the coding theory;
- In 2010. N.A.M. Al-Seraji. [3] studied the geometry of the plane of order seventeen and its application to error-correcting codes;

In 2011. B.A. Al-Zangana Emad. [4] described the geometry of the plane of order nineteen and its application to error-correcting codes;

- In 1998. Hirschfeld, J. W. P. [5] classified projective geometries over finite fields;
- In 2013. N.A.M. Al-Seraji. [6] considered an almost maximum distance separable codes;
- In (2013). N.A.M. Al-Seraji. [7] described generalized of optimal codes;
- In 2012. N.A.M. Al-Seraji. [8] studied the optimal codes;

The following results are interesting to area of research:

*Email: dr.najm@uomustansiriyah.edu.iq

Theorem 1.2 [1] (The sphere packing or Hamming bound)
A $q-ary\ (n,M,2e\ +\ 1)-code\ C$ satisfies

$$M\{\binom{n}{0}+\binom{n}{1}(q-1)+\cdots+\binom{n}{e}(q-1)^e\}\leq q^n.$$

Corollary 1.3.[1] A $q-ary\ (n,M,2e\ +\ 1)$ code C is perfect if and only if equality holds in Theorem 1.2.
Definition 1.4 [1] A $q-ary$ code C of length n is a subset of $(F_q)^n$.
Example 1.5 [1] To send just the two messages YES and NO, the following encoding suffices: $YES\ =\ 1$, $NO\ =\ 0$. If there is an error, say 1 is sent and 0 arrives, this will go undetected. So, add some redundancy: $YES\ =\ 11$, $NO\ =\ 00$. Now, if 11 is sent and 01 arrives, then an error has been detected, but not corrected, since the original messages 11 and 00 are equally plausible.
So, add further redundancy: $YES\ =\ 111$, $NO\ =\ 000$. Now, if 010 arrives, and it is supposed that there was at most one error, we know that 000 was sent: the original message was NO.

2. The classification of cubic curves over a finite field of order 3

The polynomial of degree three $g_2(x)=x^3-x-2$ is primitive in $F_3=\{0,1,2\}$, since $g_2(0)=1$, $g_2(1)=1$ and $g_2(2)=1$, also $g_2(\delta)=0$, $g_2(\delta^3)=0$, $g_2(\delta^9)=0$, this means δ,δ^3,δ^9 are roots of g_2 in F_{3^3}. The companion matrix of $g_2(x)=x^3-x-2$ in $F_3[x]$ generated the points and lines of $PG(2,3)$ as follows:

$$P(k)=[1,0,0]C(g)^{k-1}=[1,0,0]\begin{pmatrix}0&1&0\\0&0&1\\2&1&0\end{pmatrix}^{k-1},\ k=1,\dots,13\ .$$

The points of $PG(2,3)$ are :

$P(1)=[1,0,0]$	$P(2)=[0,1,0]$	$P(3)=[0,0,1]$	$P(13)=[2,0,1]$
$P(4)=[2,1,0]$	$P(5)=[0,2,1]$	$P(6)=[1,2,1]$	
$P(7)=[1,1,1]$	$P(8)=[2,2,1]$	$P(9)=[1,0,1]$	
$P(10)=[1,1,0]$	$P(11)=[0,1,1]$	$P(12)=[2,1,1]$	

With selecting the points in $PG(2,3)$ which are the third coordinate equal to zero , this means belong to $L_0=v(z)$, that is $v(z)=tz=z$ for all t in $F_3\backslash\{0\}$ and with $P(k)=k$, we obtain $L_1=\{0,1,3,9\}$, that is

$$L_k=L_1C(g)^{k-1}=L_1\begin{pmatrix}0&1&0\\0&0&1\\2&1&0\end{pmatrix}^{k-1},k=1,\dots,13$$

The lines of $PG(2,3)$ are:

ℓ_1	0	1	3	9
ℓ_2	1	2	4	10
ℓ_3	2	3	5	11
ℓ_4	3	4	6	12
ℓ_5	4	5	7	0
ℓ_6	5	6	8	1
ℓ_7	6	7	9	2
ℓ_8	7	8	10	3
ℓ_9	8	9	11	4
ℓ_{10}	9	10	12	5
ℓ_{11}	10	11	0	6
ℓ_{12}	11	12	1	7
ℓ_{13}	12	0	2	8

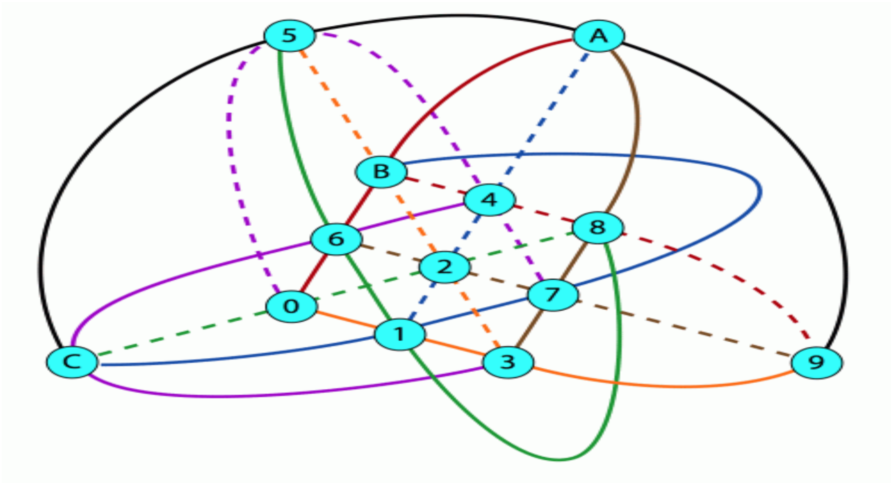

Figure 1-Drawing of $\boldsymbol{PG(2,3)}$

In the following theorem the parameters n, M and d are constructed.

Theorem 2.1: The projective plane of order three is a code with a parameters $[n = 13, M = 3^{10}, d = 4]$.

Proof: The plane π_3 has an incidence matrix $A = (aij)$, where

$$a_{ij} = \begin{cases} 1 & if \quad P_j \in \ell_i, \\ 0 & if \quad P_j \notin \ell_i. \end{cases}$$

	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}	P_{13}
ℓ_1	1	1	0	1	0	0	0	0	0	1	0	0	0
ℓ_2	0	1	1	0	1	0	0	0	0	0	1	0	0
ℓ_3	0	0	1	1	0	1	0	0	0	0	0	1	0
ℓ_4	0	0	0	1	1	0	1	0	0	0	0	0	1
ℓ_5	1	0	0	0	1	1	0	1	0	0	0	0	0
ℓ_6	0	1	0	0	0	1	1	0	1	0	0	0	0
ℓ_7	0	0	1	0	0	0	1	1	0	1	0	0	0
ℓ_8	0	0	0	1	0	0	0	1	1	0	1	0	0
ℓ_9	0	0	0	0	1	0	0	0	1	1	0	1	0
ℓ_{10}	0	0	0	0	0	1	0	0	0	1	1	0	1
ℓ_{11}	1	0	0	0	0	0	1	0	0	0	1	1	0
ℓ_{12}	0	1	0	0	0	0	0	1	0	0	0	1	1
ℓ_{13}	1	0	1	0	0	0	0	0	1	0	0	0	1

Let

$z = [0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]$

u = [1 1 1 1 1 1 1 1 1 1 1 1 1]

$w = [2\ 2\ 2\ 2\ 2\ 2\ 2\ 2\ 2\ 2\ 2\ 2\ 2]$

$m_i = u + \ell_i$.

That is,

m_1	2	2	1	2	1	1	1	1	1	2	1	1	1
m_2	1	2	2	1	2	1	1	1	1	1	2	1	1
m_3	1	1	2	2	1	2	1	1	1	1	1	2	1
m_4	1	1	1	2	2	1	2	1	1	1	1	1	2
m_5	2	1	1	1	2	2	1	2	1	1	1	1	1
m_6	1	2	1	1	1	2	2	1	2	1	1	1	1
m_7	1	1	2	1	1	1	2	2	1	2	1	1	1
m_8	1	1	1	2	1	1	1	2	2	1	2	1	1
m_9	1	1	1	1	2	1	1	1	2	2	1	2	1
m_{10}	1	1	1	1	1	2	1	1	1	2	2	1	2
m_{11}	2	1	1	1	1	1	2	1	1	1	2	2	1
m_{12}	1	2	1	1	1	1	1	2	1	1	1	2	2
m_{13}	2	1	2	1	1	1	1	1	2	1	1	1	2

$v_i = w + \ell_i$

That is,

v_1	0	0	2	0	2	2	2	2	2	0	2	2	2
v_2	2	0	0	2	0	2	2	2	2	2	0	2	2
v_3	2	2	0	0	2	0	2	2	2	2	2	0	2
v_4	2	2	2	0	0	2	0	2	2	2	2	2	0
v_5	0	2	2	2	0	0	2	0	2	2	2	2	2
v_6	2	0	2	2	2	0	0	2	0	2	2	2	2
v_7	2	2	0	2	2	2	0	0	2	0	2	2	2
v_8	2	2	2	0	2	2	2	0	0	2	0	2	2
v_9	2	2	2	2	0	2	2	2	0	0	2	0	2
v_{10}	2	2	2	2	2	0	2	2	2	0	0	2	0
v_{11}	0	2	2	2	2	2	0	2	2	2	0	0	2
v_{12}	2	0	2	2	2	2	2	0	2	2	2	0	0
v_{13}	0	2	0	2	2	2	2	2	0	2	2	2	0

The remain vectors of code C are constructed combination of z, u, w, ℓ_i, m_i and v_i where $i = 1, \ldots, 13$, Note that $d(l_i, l_j)$ = number of points on exactly one of l_i or l_j. Then

$d(z, \ell_i) = 4$	$d(u, m_i) = 4$
$d(u, \ell_i) = 9$	$d(z, v_i) = 9$
$d(w, \ell_i) = 13$	$d(z, m_i) = 13$
$d(\ell_i, m_i) = 10$	$d(u, v_i) = 13$
$d(\ell_i, v_i) = 13$	$d(\ell_i, \ell_j) = 6, i \neq j$
$d(m_i, v_i) = 13$	$d(m_i, m_j) = 6, i \neq j$
$d(u, z) = 13$	$d(v_i, v_j) = 6, i \neq j$
$d(u, w) = 13$	$d(\ell_i, m_j) = 10, i \neq j$
$d(z, w) = 13$	$d(\ell_i, v_j) = 10, i \neq j$

If we substitute the values of $n = 13, d = 4$, $e = 1$, in inequality of theorem 1.2, we get $M = 3^{10}$. Hence C is a $(13, 3^{10}, 4)$-code.

$$3^{10}\left\{\binom{13}{0} + \binom{13}{1}(3-1)\right\} = 3^{10}(1 + 26) = 3^{10}.3^3 = 3^{13}.$$

By Corollary 1.3,therefor C is perfect. ■

The goal of the following theorem is to show that the code C is closed under the operation of addition modulo 3:

Theorem 2.2: The code $C = [n = 13, M = 3^{10}, d = 4]$ which is derived from the projective plane of order three is linear; that is, the sum modulo 3 of any two element of C is in C.

Proof: Here is the geometry with $P_i = i$. Where $i = 1, \dots, 13$.

Then $\ell_i + \ell_j = a_i$, where $i, j = 1, \dots, 13$. such that

$a_r = 1 \iff P_r$ lies on precisely one of, ℓ_i, ℓ_j and

$a_r = 0 \iff P_r$ lies on the third line through $\ell_i \cap \ell_j$.

Here $\ell_i + \ell_j$, $\ell_i + u$, $\ell_i + w$, $\ell_i + m_i$, $\ell_i + v_i$ in C.

$m_i + m_j$, $m_i + u$, $m_i + w$, $m_i + v_i$ in C.

$v_i + v_j$, $v_i + u$, $v_i + w$ in C. ■

References

1. Hirschfeld, J.W.P. **2014.** *Coding Theory*, Lectures, Sussex University, UK.
2. Hill, R. **1986.** *A first course in coding theory*, Clarendon Press, Oxford.
3. Al-Seraji. N.A.M. **2010.** The Geometry of The Plane of order Seventeen and its Application to Error-correcting Codes, Ph.D. Thesis, University of Sussex, UK.
4. Al-Zangana Emad, B.A. **2011.** The Geometry of The Plane of order Nineteen and its Application to Error-correcting Codes, Ph.D. Thesis, University of Sussex, UK.
5. Hirschfeld, J. W. P. **1998.** *Projective geometries over finite fields*. 2nd Edition, Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, New York.
6. Al-Seraji, N.A.M. **2013**. On Almost Maximum Distance Separable codes, Iraq journal of Science, **54**(3).
7. Al-Seraji, N.A.M. **2013.** Generalized of Optimal Codes, *AL-Mustansiriyah Journal of Science*, **24**(6).
8. Al-Seraji, N.A.M. **2012.** On Optimal Codes, *AL-Mustansiriyah Journal of Science*, **23**(6).